This presentation is intended only for use by Tulane University faculty, staff, and students. No copy or use of this presentation should occur without the permission of Tulane University. Tulane University retains all intellectual property interests associated with the presentation. Tulane University makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.
Tulane University and Health Sciences Center

HIPAA – Privacy & Security
(Part 1 & Part 2)

HITECH
(Part 3)

Revised 3/23/2011
Two (2) parts of HIPAA covered in this presentation:

• **HIPAA Privacy** – Protection for the privacy of Protected Health Information (PHI) effective April 14, 2003 (including Standardization of electronic data interchange in health care transactions, effective October 2003)

• **HIPAA Security** – Protection for the security of electronic Protected Health Information (e-PHI) effective April 20, 2005
What is the difference between Privacy and Security?

- The **Privacy Rule** sets the standards for how covered entities and business associates are to maintain the privacy of Protected Health Information (PHI).
- The **Security Rule** defines the standards which require covered entities to implement basic safeguards to protect electronic Protected Health Information (e-PHI).
Part 1:

HIPAA Privacy Training

Revised 3/23/2011
The Health Insurance Portability and Accountability Act (HIPAA) requires that Tulane University, including the Health Sciences Center, train all workforce members of “Covered Entities” on the HIPAA policies and…
...those specific HIPAA-required Procedures that may affect the work you do for the University and the Health Sciences Center.
The HIPAA Training Program will help you to understand:

- What is HIPAA?
- Who has to follow the HIPAA law?
- When is the HIPAA implementation date?
- How does HIPAA affect you and your job?
- Why is HIPAA important?
- Where can you get answers to your questions about HIPAA?
What is HIPAA?

- HIPAA is the Health Insurance Portability and Accountability Act of 1996.
- HIPAA is a Federal Law.

- HIPAA is a response, by Congress, to healthcare reform.
- HIPAA affects the health care industry.
- HIPAA is mandatory.
HIPAA ...

- Protects the privacy and security of a patient’s health information.
- Provides for electronic and physical security of a patient’s health information.
- Prevents health care fraud and abuse.
- Simplifies billing and other transactions, reducing health care administrative costs.
Who must follow the HIPAA Law?

At the Tulane University and Health Sciences Center, Covered Entities must follow the HIPAA Law.
The Tulane Covered Entity

The Covered Health Care Component (Entity) consists of the Tulane University Medical Group, its participating physicians and clinicians, and all University employees and departments that provide management, administrative, financial, legal and operational support services to or on behalf of Tulane University Medical Group to the extent that such employees and departments use and disclose individually identifiable health information in order to provide these services to the TUMG, and would constitute a “business associate” of Tulane University Medical Group if separately incorporated.
A Business Associate is…

• A person or entity which performs certain functions, activities, or services for or to the Tulane University Medical Group involving the use and/or disclosure of PHI, but the person or entity is not a part of TUMG or its workforce. (Examples: transcription services, temporary staffing services, record copying company.)

• The Tulane University Medical Group is required to have agreements with business associates that protect a patient’s PHI.
Covered Entity...Always

Once you are part of a covered entity, you are a covered entity with respect to all Protected Health Information (PHI), whether it is transmitted electronically, in paper format, or transmitted orally.
Covered Entity?

- The key is whether any of the Covered Transactions are performed electronically
Examples of Covered Entities

- Providers
- Health Plans
- Clearinghouses for Electronic Billing
- Business Associates (through contracts)
Covered Transactions Consist of

- Enrollment and dis-enrollment
- Premium payments
- Eligibility
- Referral certification and authorization
- Health claims
- Health care payment and remittance advice
What Patient Information Must We Protect?

• Protected Health Information (PHI)
  ➢ Relates to past, present, or future physical or mental condition of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
  ➢ Is transmitted or maintained in any form (electronic, paper, or oral representation).
  ➢ Identifies, or can be used to identify the individual.
Examples of PHI
PHI = Health Information with Identifiers

- Name
- Address (including street, city, parish, zip code and equivalent geocodes)
- Name of employer
- Any date (birth, admit date, discharge date)
- Telephone and Fax numbers
- Electronic (email) addresses
- Social Security Number
- Medical Records
Tulane University’s Covered Entity…

…may not use or disclose an individual’s protected health information, except as otherwise permitted, or required, by law.
But…

Tulane University’s Covered Entity MAY Use and Share a Patient’s PHI for

- Treatment of the patient, including appointment reminders
- Payment of health care bills
And for…

- Business and management operations
- Disclosures required by law
- Public Health and other governmental reporting
“Treatment” Includes…

- Direct patient care
- Coordination of care
- Consultations
- Referrals to other health care providers
“Payment” Includes any activities required to bill and collect for health care services provided to patients.

“Health Care Operations” Includes business management and administrative activities, quality improvement, compliance, competency, and training.
Tulane University’s Covered Entity

- Must use or share only the minimum amount of PHI necessary, except for requests made
  - for treatment of the patient
  - by the patient, or as requested by the patient to others
  - by the Secretary of the Department of Health & Human Services (DHHS)
  - as required by law
  - to complete standardized electronic transactions, as required by HIPAA
For many other uses and disclosures of PHI... the Tulane University Covered Entity must get a signed authorization from the patient (for example, to disclose PHI to a pharmaceutical company).
The Authorization MUST

• Describe the PHI to be used or released
• Identify who may use or release the PHI
• Identify who may receive the PHI
• Describe the purposes of the use or disclosure
• Identify when the authorization expires
• Be signed by the patient or someone making health care decisions (personal representative) for the patient (as per Policy GC-022)
HIPAA Requires

Tulane University’s Covered Entity to:

• Give each patient a Notice of Privacy Practices that describes:
  - how the Tulane University Medical Group can use and share his or her Protected Health Information (PHI)
  - a patient’s privacy rights

• Request every patient to sign a written acknowledgement that he/she has received the Notice of Privacy Practices.
Patient Rights

- The right to **request restriction** of PHI uses & disclosures
- The right to **request alternative** forms of **communications** (mail to P.O. Box, not street address; no message on answering machine, etc.)
- The right to **access and copy** patient’s PHI
- The right to an **accounting of the disclosures of PHI**
- The right to request **amendments to information**
The **Notice of Privacy Practices** explains what the Tulane University Covered Entity can do with PHI

To get your copy…

Visit the HIPAA Privacy Practices website at [http://tulane.edu/counsel/upco/privacy-policies.cfm](http://tulane.edu/counsel/upco/privacy-policies.cfm) or

Call the Privacy Official at 504-988-7739 to request a copy or ask questions.
When Does Tulane University Covered Entity Have to Protect PHI?

NOW!
NOW!
NOW!

Privacy Compliance went into effect on April 14, 2003.
How does HIPAA affect MY job?
Well, if...

- You currently see, use, or share a person’s PHI as a part of your job, HIPAA may change the way you do your job
- You currently work directly with patients, HIPAA may change the way you do your job

As part of your job, you must protect the privacy of the patient’s PHI
When can you use PHI?

Only to do your job!
At all times…

Protect a patient’s information as if it were your own!

- Look at a patient’s PHI only if you need it to perform your job.
- Use a patient’s PHI only if you need it to perform your job.
- Give a patient’s PHI to others only when it’s necessary for them to perform their jobs.
- Talk to others about a patient’s PHI only if it is necessary to perform your job, and do it discreetly.
For Example…

1. You are a physician whose friend’s wife is in a coma in the hospital after an accident. He asks you to review the admitting physician’s orders and see if you concur. What can you legally do under HIPAA?

A. You can look at her chart so you can answer your friend’s questions about his wife’s condition.

B. You can ask the charge nurse on the floor to look into her records for you.

C. You can tell your friend that you can only look at his wife’s medical records if her physician, the patient, or in this case, the patient’s representative, allows you to do so. Suggest that your friend ask to discuss her treatment and progress with the attending physician.
Answer:

C. Under HIPAA, you are only allowed to use information required to do your job. Since you are neither the attending physician nor part of the patient’s care team, it is against the law to access the patient record or ask someone to access it on your behalf—even though you may know the person and just want to be helpful. Remember that, if you were in a similar situation, you might not want your colleagues going through your own medical records, or those of your spouse or close friend.
Public Viewing / Hearing of PHI

• Refrain from discussing PHI in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients.

• Medical and support staff should take care of sharing PHI with family members, relatives, or personal representatives of patients. Information cannot be disclosed unless the patient has had an opportunity to agree with or object to the disclosure.

• Personal representatives are those individuals who, under Louisiana law, are able to make healthcare decisions on behalf of the patient.
For Example

Dr. Fortissimo was eating breakfast in the Med School Cafeteria one Monday morning, and talking on his cell phone to another doctor. During the conversation, he referred to the patient by name, and described her diagnosis. The cafeteria worker at the next table heard the call. What could have been done differently to protect the patient’s privacy?

A. The patient’s privacy was protected; nothing was done wrong, since no PHI was mentioned.

B. It is important to be aware of your surroundings when you discuss patient information (PHI). The patient’s case should have been discussed in a more private location, or, at least, in a low voice that could not be overheard.

C. Other customers should not be allowed to eat in that section of the cafeteria so as to avoid such situations.
B. Although HIPAA allows incidental uses and disclosures, this type of disclosure is not allowed. PHI includes oral communications. The patient’s case should only have been discussed in a location that provided for the privacy of the information discussed.
Use and Disclosures of PHI for Research

- The I.R.B. (Institutional Review Board) may not authorize the use or disclosure of PHI for research purposes except:
  - For reviews preparatory to research;
  - For research on the protected health information of a decedent;
  - If the information is completely “de-identified”;
  - If the information is partially de-identified into a “limited data set” and the recipient of the information signs a data use agreement to protect the privacy of such information;
Uses and Disclosures of PHI for Research (continued)

- If Tulane University Medical Group has obtained a valid authorization from the individual subject of the information; or
- If the I.R.B. approves a waiver of the individual authorization requirement (Policy GC-012)
Use of PHI in Research
(continued)

If you have any questions concerning Use and Disclosures of PHI for Research (Policy GC-012), call the I.R.B. at 504-988-2665, the Privacy Official at 504-988-7739, or the Associate General Counsel at 504-988-5031.
Uses and Disclosures of PHI for Fundraising

- The Tulane University Health Care Component may use, or disclose to a business associate or to an institutionally-related foundation, the following protected health information for the purpose of raising funds for its own benefit, without an authorization:
  - Demographic information related to an individual; and
  - Dates of health care provided to an individual.

- The Tulane University Health Care Component must include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving any further fundraising communications.
Uses and Disclosures of PHI for Fundraising
(continued)

• The Tulane University Health Care Component must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.

• The Business Associates and/or Sr. Associate Vice President of Advancement for the Health Sciences Center shall maintain a list of all patients who have opted out and provide a copy of said list annually to the Privacy Official of the General Counsel’s Office.

• The use of Protected Health Information (PHI) for fundraising purposes other than as described herein is prohibited without a patient authorization, which meets the requirements of policy GC-003.
Uses and Disclosures of PHI for Marketing

- A Tulane University Medical Group health care provider may use PHI to communicate to the patient about a health-related product or service the TUMG provides.
- A TUMG health care provider may use PHI to communicate to the patient about general health issues: disease prevention, wellness classes, etc.
- For all other marketing, a patient authorization must be obtained, unless the communication is in the form of
  - A face-to-face communication made by TUMG to an individual
  - A promotional gift of nominal value provided by TUMG
For Example…

- A physician, while having a new-product orientation meeting with a drug company rep., learns about a new COX-2 inhibitor being developed by the pharmaceutical company. The physician provides the rep with the names and phone numbers of a few of his patients with arthritis, because he believes that they could benefit from the new treatment. A week later, patients call the doctor’s office complaining about being solicited by the drug company to take part in a clinical trial.
What does HIPAA say about this practice?

A. Since the physician had good intentions, this situation should not be avoided, and the doctor has not violated HIPAA.

B. Physicians should stop meeting with drug company reps, as there are many circumstances that could result in violations of federal law, including HIPAA.

C. Since PHI was disclosed for purposes other than what state and federal law allows without a patient’s authorization, an authorization from the patients should have been obtained before the PHI was released.
c. PHI was disclosed without patient authorization. Never provide information to a friend, colleague, or business representative UNLESS it is required as part of your job and permitted under HIPAA and/or other state and federal laws. Always keep your patient’s information confidential to maintain your rapport and the patient’s trust. Providing an unauthorized release of information to a drug rep for marketing or research purposes violates state and federal law.
How Do I Know if HIPAA Affects My Job?

1. The Administration of the Tulane University Covered Entity has determined what departments are covered under HIPAA. The managers of those departments, along with the Privacy Official and Legal Counsel, have determined what positions in each department are covered.

2. Job descriptions reflect the HIPAA verbiage:
“Employee provides services associated to the Tulane University Medical Group, its participating physicians and clinicians, which is a covered entity under the HIPAA rule. In the scope of performing functions, including but not limited to management, administrative, financial, legal and operational support services, I may have access to Protected Health Information (PHI), which is information, whether oral, written, electronic, visual, pictorial, physical, or any other form, that relates to an individual’s past, present or future physical or mental health status, condition, treatment, service, products purchased, or provision of health care and which reveals the identity of the individual, whose health care is the subject of the information, or where there is reasonable basis to believe such information could be utilized to reveal the identity of that individual: ( ) Yes ( ) No”
You, as an employee, must sign your job description, answering “yes” or “no” to the HIPAA statement.

If you have any questions, ask your manager, or call the Privacy Official at 504-988-7739.
Why is protecting privacy and security important?

• We all want our privacy protected when we are patients – it’s the right thing to do.
  ➢ Don’t be careless or negligent with PHI in any form.

• HIPAA and Louisiana law require us to protect a patient’s privacy.
What if there is a breach of confidentiality?

- Breaches of the policies and procedures or a patient’s confidentiality must be reported to the Tulane University Privacy Official at 504-988-7739.
- Tulane’s policy (GC-009) states,
  - “Anyone who knows or has reason to believe that another person has violated this policy should report the matter promptly to his or her supervisor or the University’s Privacy Official.”
...and if a breach is reported

- The incident will be thoroughly investigated.
- The Tulane University Covered Entity is required to attempt to remedy the harmful effects of any breach.
Tulane University’s Covered Entity is serious about protecting our patients’ privacy.

Policy GC-009 states,

“The Tulane University Health Care Component is committed to protecting the privacy and confidentiality of health information about its patients. Protected health information is strictly confidential and should never be given, nor confirmed to anyone who is not authorized under the Tulane University Health Care Component policies or applicable law to receive this information.”
Disciplinary Actions

• Internal Disciplinary Actions
  ➢ Individuals who breach the policies will be subject to appropriate discipline under Policy GC-009.

• Civil Penalties
  ➢ Covered entities and individuals who violate these standards will be subject to civil liability.

An employee who does not protect a patient’s privacy could lose his or her job!
Penalties are

- $100 per violation
- $25,000 for an identical violation within one year
- $50,000 for wrongful disclosure
- $100,000 and/or 5 years in prison for wrongful violation for obtaining PHI under false pretenses
- $250,000 and/or 10 years in prison if committed with intent to sell or transfer for commercial advantage, personal gain, or malicious harm, includes obtaining or disclosing.
Protecting Patient Privacy Requires Us to Secure Patient Information
Employees should not download, copy, or remove from the clinical areas any PHI, except as necessary to perform their jobs.

Upon termination of employment, or upon termination of authorization to access PHI, the employee **must** return to the University all copies of PHI in his or her possession.
Faxing

• Faxing is permitted. Always include, with the faxed information, a cover sheet containing a Confidentiality Statement:
  
  ➢ The documents accompanying the transmission contain confidential privileged information. The information is the property of the Tulane University Medical Group and intended only for use by the individual or entity named above. The recipient of this information is prohibited from disclosing the contents of the information to another party.

  ➢ If you are neither the intended recipient, or the employee or agent responsible for delivery to the intended recipient, you are hereby notified that disclosure of contents in any manner is strictly prohibited. Please notify [name of sender] at [facility name] by calling [phone #] immediately if you received this information in error.
Limit manual faxing to urgent transmittals:

- Medical emergencies
  - Faxing PHI is appropriate when the information is needed immediately for patient care
- Other situations considered urgent (e.g., results from lab to physician)
Information that **should not** be faxed (except in an emergency):

- Drug dependency
- Alcohol dependency
- Mental illness or psychological information
- Sexually-transmitted disease (STD) information
- HIV status
Locating a Fax Machine

- Location should be secure whenever possible,
- In an area that is not accessible to the public, and
- Whenever possible, in an area that requires security keys or badges for entry.
If information is inadvertently faxed to a patient-restricted party or a recipient where there is a risk of release of the PHI (e.g., newspaper), the Privacy Official should be notified (504-988-7739), and legal counsel should become involved.
Public Viewing/Hearing

• PHI should not be left in conference rooms, out on desks, or on counters where the information may be accessible to the public, or to other employees or individuals who do not have a need to know the protected health information.
Treat a Patient’s Information as if it were your own …

Tulane University’s Covered Entity Needs Your Help in Protecting Our Patients’ Privacy.
In Review…

- Tulane University Medical Group is a Covered Entity under HIPAA
- TUMG has specific policies relating to HIPAA
  – *And Remember*…
- TUMG has areas outside of the main campus that are subject to HIPAA (e.g., Northshore clinics)
HIPAA Privacy Policies and Procedures

All HIPAA Privacy Policies and Procedures are located on the University Privacy and Contracting Office’s website:

http://tulane.edu/counsel/upco/privacy-policies.cfm
Part 2:

HIPAA Security Training
So, what *IS* “e-PHI”?

• **e-PHI** (electronic Protected Health Information) is computer-based patient health information that is *used, created, stored, received or transmitted* by Tulane using any type of electronic information resource.

• Information in an electronic medical record, patient billing information transmitted to a payer, digital images and print outs, information when it is being sent by Tulane to another provider, a payer or a researcher.
How do we protect e-PHI?

- Ensure the *confidentiality, integrity, and availability* of information through safeguards (Information Security)
- Ensure that the information will not be disclosed to unauthorized individuals or processes (*Confidentiality*)
- Ensure that the condition of information has not been altered or destroyed in an unauthorized manner, and data is accurately transferred from one system to another (*Integrity*)
- Ensure that information is accessible and usable upon demand by an authorized person (*Availability*)
Good Computing Practices: Safeguards for Users
Safeguard #1: Access Controls (Unique User Identification)

- Users are assigned a unique “User ID” for log-in purposes, which limits access to the minimum information needed to do your job. *Never use anyone else’s log-on, or a computer someone else is logged-on to.*
- Use of information systems is audited for inappropriate access or use.
- Access is cancelled for terminated employees.
Safeguard #2: Password Protection

Tulane University requires that:

- All passwords be **changed at least once every 6 months**, or immediately if a breach of a password is suspected;
- User accounts that have system-level privileges granted through group memberships or programs have a unique password from all other accounts held by that user;
- Passwords not be inserted into email messages or other forms of electronic communication;
- Personal Computers and other portable devices such as Laptops and PDAs which may contain e-PHI must be password protected, and encrypt the e-PHI;
- Default vendor passwords be changed immediately upon installation of hardware or software;
If I think someone knows my password?

- **Notify the Help Desk** or your computer support person, and notify the Information Systems Office.
- **Change your password IMMEDIATELY** (if you need assistance, ask the Help Desk)

**Remember:** You are responsible for everything that occurs under your Tulane login.
Safeguard #3: E-mail Encryption

1. Email Encryption to HCA Healthcare
2. Email Encryption to the outside world
3. Email Encryption within Tulane
Email Encryption to HCA Healthcare

Email messages between tulane.edu and hcahealthcare.com are encrypted automatically by servers policy.
Email Encryption to the outside world

- Type the word Secure: at the subject line
- It can be lowercase, uppercase or mix case
- It can be anywhere in the subject line
  - Secure:
  - secure:
  - SECURE:
  - The Colon “:” is important.
Email Encryption to the outside world

- For Microsoft Outlook, you can also set the message sensitivity to Confidential
Email Encryption within Tulane

For Outlook Client 2007
Email Encryption within Tulane

By default, email within Tulane for other clients such as Mac Mail, Entourage or iPhone are encrypted with SSL.
Safeguard #4: Workstation Security
Workstation Security (continued)

• “Workstations” includes electronic computing devices, laptops or desktop computers, or other devices that perform similar functions, and electronic media stored in or near them

• “Physical Security Measures” include
  – Disaster Controls
  – Physical Access Controls
  – Device and Media Controls

• “Malware Controls” are measures taken to protect against any software that causes unintended results
Disaster Controls

- Protect workstations from natural and environmental hazards
- Locate equipment above ground level to protect it against flood damage
- Use electrical surge protectors
- Move workstations away from overhead sprinklers
Access Controls

- **Log-off** before leaving a workstation unattended. This will prevent other individuals from accessing e-PHI under your User-ID, and limit access by unauthorized users.
Workstation Security (continued)

- **Lock-up!**:
  - Offices, windows, sensitive papers and PDAs, laptops, mobile devices/media
  - Lock your workstation
  - Encryption tools should be implemented when physical security cannot be provided
  - Maintain key control
Device Controls

- **Auto Log-Off**: Where possible and appropriate, devices must be set to “lock” or “log-off” and require a user to sign in again after **5 minutes**
- **Automatic Screen Savers**: Password protect, and set to activate in **5 minutes**
Malware – a few bad examples

• Viruses
  – are programs that attempt to spread throughout your system and the entire network
  – can be prevented by installing antivirus software on your computer, and updating it frequently
Worms...

- spread without any user action. They take advantage of security holes in the operating system or software package
- can be prevented by making sure that your system has all security updates installed
Spyware...

- is a class of programs that monitors your computer usage habits and reports them for storage in a marketing database
- are installed without you knowing while installing another program or browsing the Internet
- can open advertising windows
- can be prevented by installing and running an updated spyware scanner
Keystroke Loggers…

- can be software (programs that log every keystroke typed) or hardware (devices installed between your keyboard and computer)
- can be detected by most antivirus programs and spyware scanners
- can be spotted if you check your hardware for anything unfamiliar (do it often)
Remote Access Trojans...

• allow remote users to connect to your computer without your permission, letting them
  – take screenshots of your desktop
  – take control of your mouse and keyboard
  – access your programs at will
• can be detected by most antivirus programs
Suspicious Email includes...

- any email you receive with an attachment
- any email from someone whose name you do not recognize
- Phishing
Indication of tampered accounts...

• your account is locked when you try to open it
• your password isn’t accepted
• you’re missing data
• your computer settings have mysteriously changed

If you suspect someone has tampered with your account, call the Help Desk.
Signs of Malware are…

- Reduced performance (your computer slows or “freezes”)
- Windows opening by themselves
- Missing data
- Slow network performance
- Unusual toolbars added to your web browser

Contact the Help Desk if you suspect that your computer has malware installed.
Acceptable Use of Computers

- End Users (read “YOU-ALL”) are responsible for any violations associated with their User ID
- Use of computer system must be consistent with Tulane’s goals
- All computer equipment and electronic data created by it belong to the University
End users must comply…

- with all Federal and State laws
- with organizational rules and policies
- with terms of computing contracts
- with software licensing rules

And must take reasonable precautions to avoid introducing computer viruses into the network, and must participate and cooperate with the protection of IT infrastructure.
And Thou shall not...

- Engage in any activity that jeopardizes the availability, performance, integrity, or security of the computer system
- Use computing resources wastefully
- Use IT resources for personal gain or commercial activities not related to your job
- Install, copy, or use any software in violation of licensing agreements, copyrights, or contracts
Or …

- Try to access the files or email of others unless authorized by the owner
- Harass, intimidate, or threaten others through e-messages
- Construct a false communication that appears to be from someone else
- Send or forward unsolicited email to lists of people you don’t know
- Send, forward, or reply to email chain letters
- Send out “Reply to all” mass emailings
Or...

- Create or transmit offensive, obscene, or indecent images, data, or other material
- Re-transmit virus hoaxes
Because...

Engaging in these activities could result in disciplinary action up to, and including, loss of network access, termination of employment, and civil or criminal liability.
Safeguard #5: Workstation Security – Check List

Always use the physical security measures listed in Safeguard #4, including this “Check List”

• Use an Internet Firewall, if applicable
• Use Anti-virus software, and keep it up-to-date
• Install computer software updates, such as Microsoft patches
• Encrypt and password-protect portable devices (PDAs, laptops, etc.)
• Lock-it-up! Lock office or file cabinets, lock up laptops
• Use automatic log-off from programs
• Use password-protected screen savers
• Back up critical data and software programs
Safeguard #5: Workstation Security – When you take it with you…

Security for USB Memory Sticks and Storage Devices:

• Don’t store e-PHI on memory sticks
• If you must store it, either de-identify it, or encrypt it
• Delete the e-PHI when no longer needed
• Protect the devices from loss and damage
Safeguard #5: Workstation Security — PDAs

- Don’t store e-PHI on PDAs
- If you **must** store it, de-identify it; or
- Encrypt it and password-protect it
- Back up original files
- Synchronize with computers as often as practical
- Delete e-PHI files from all portable media when no longer needed
- Protect your device from loss or theft
Safeguard #6: Data Management and Security
Data Management and Security

Data Storage

Portable Devices:

- Permanent copies of e-PHI should not be stored on portable equipment, such as laptop computers, PDAs, and memory sticks (heard this before?)
- If necessary, temporary copies can be used on portable computers only while using the data, and if encrypted to safeguard the data if the device is lost or stolen
Data Management and Security

Data Disposal

Destroy e-PHI data which is no longer needed:

- Know where to take hard drives, CDs, zip disks, or any backup devices for appropriate safe disposal or recycling (like to your IT professional)
Security Incidents and e-PHI
(HIPAA’s Final Security Rule)

A “Security Incident” is

“The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” [45 CFR 164.304]
Reporting Security Incidents / Breaches:

You are required to:

• Respond to security incidents and security breaches, and report them to:
  ➢ Security Official – Hunter Ely 504-988-8566
  ➢ Privacy Official – Glenda Folse 504-988-7739
Security Reminders!

- Password protect your computers and devices
- Backup your electronic Protected Health Information
- Keep offices secured
- Keep portable storage locked up
- Patch your systems
- Run anti-virus, anti-spy ware
- Encrypt your e-PHI, if applicable
- Help Desk Phone # 504-862-8888 Uptown ext. 88888 from HSC
Security Reminders! (continued)

Good Security Standards follow the “90 / 10” Rule:

- 10% of security safeguards are technical
- 90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices
  - Example: The lock on the door is the 10%. Your responsibility is 90% which are remembering to lock, checking to see if it is closed, ensuring others do not prop the door open, keeping controls of keys. 10% security is worthless without YOU!
Some safeguards for computer users:

- User Access Controls.......................... TS-34
- Passwords........................................... TS-15
- Workstation Security............................ TS-28
- Portable Device Security....................... TS-28
- Data Management............................... TS-33
  - Backup, archiving, restoring
- Recycling Electronic Medias and Computers.......................... TS-30
- Reporting Security Incidents/Breaches.....
Resources …

…for HIPAA Privacy information:
• Web site: http://tulane.edu/counsel/upco/
• HIPAA Policies and Procedures
• Privacy Official: Glenda Folse 504-988-7739

… for HIPAA Security information:
• Web site: http://tulane.edu/compliance/
• HIPAA Security Policies: http://www.tulane.edu/~hipaa/
• Security Official: Hunter Ely 504-988-8566
Part 3:

Health Information Technology for Economic and Clinical Health Act (HITECH)

Revised 3/23/2011
HITECH-Overview

- HITECH is a part of the American Recovery and Reinvestment Act of 2009
- It is a federal law that affects the healthcare industry
- Act allocated ~$20 billion to health information technology projects, expanded the reach of HIPAA by extending certain obligations to business associates and imposed a nationwide security breach notification law
HITECH-Breach Notification Provisions

- One of the biggest changes in HITECH is the inclusion of a federal breach notification law for health information
  - Many states, including LA, have data breach laws that require entities to notify individuals
  - State laws typically only pertain to personal information (which does not necessarily include medical information)
HITECH-Breach Notification Provisions

- The law requires covered entities and business associates to notify individuals, the Secretary of Health and Human Services and, in some cases, the media in the event of a breach of unsecured protected health information
  - The law applies to the Tulane Health Care Component, which consists of the Tulane University Medical Group (“TUMG”), its participating physicians and clinicians, and all Tulane University employees and departments that provide management, administrative, financial, legal and operational support services to or on behalf of TUMG to the extent that such employees and departments use and disclose individually identifiable health information in order to provide these services to TUMG, and would constitute a “business associate” of TUMG if separately incorporated.
  - A business associate is a person or entity that performs certain functions or services for or to TUMG involving the use and/or disclosure of PHI, but the person or entity is not part of TUMG or its workforce (examples include law firms, transcription services and record copying companies).
HITECH-Breach Notification Provisions

• All workforce members of the Tulane Health Care Component must be trained to ensure they are aware of the importance of timely reporting of privacy and security incidents and of the consequences of failing to do so.

• Compliance Date: September 23, 2009
HITECH-Breach Notification Provisions

- Law applies to breaches of “unsecured protected health information”
  - **Protected Health Information (PHI)**
    - Relates to past, present, or future physical or mental condition of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
    - Is transmitted or maintained in any form (electronic, paper, or oral representation).
    - Identifies, or can be used to identify the individual.
    - Examples of PHI include
      - Health information with identifiers, such as name, address, name of employer, telephone number, or SSN
      - Medical Records including medical record number, x-rays, lab or test results, prescriptions or charts
  - **Unsecured**
    - Information must be encrypted or destroyed in order to be considered “secured”
Definition of “Breach”

1. Was there an impermissible acquisition, access, use or disclosure not permitted by the HIPAA Privacy Rule?
   • Examples include
     – Laptop containing PHI is stolen
     – Receptionist who is not authorized to access PHI looks through patient files in order to learn of a person’s treatment
     – Nurse gives discharge papers to the wrong individual
     – Billing statements containing PHI mailed or faxed to the wrong individual/entity
2. Did the impermissible use or disclosure under the HIPAA Privacy Rule compromise the security or privacy of PHI?

- Is there a significant risk of financial, reputational or other harm to the individual whose PHI was used or disclosed?
  - If the nature of the PHI does not pose a significant risk of financial, reputational, or other harm, then the violation is not a breach. For example, if a covered entity improperly discloses PHI that merely included the name of an individual and the fact that he received services from a hospital, then this would constitute a violation of the Privacy Rule; but it may not constitute a significant risk of financial or reputational harm to the individual. In contrast, if the information indicates the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the PHI includes information that increases the risk of identity theft (such as a social security number, account number, or mother’s maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.

- Tulane is responsible for conducting risk assessment and should be fact specific
3. **Exceptions** to a Breach

- Unintentional acquisition, access, use or disclosure by a workforce member (“employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity”) acting under the authority of a covered entity or business associate
  
  - Example: billing employee receives and opens an e-mail containing PHI about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices he is not the intended recipient, alerts the nurse of the e-mail and then deletes it. The billing employee unintentionally accessed PHI to which he was not authorized to have access. However, the billing employee’s use of the information was done in good faith and within the scope of authority, and therefore, would not constitute a breach and notification would not be required, provided the employee did not further use or disclose the information accessed in a manner not permitted by the Privacy Rule.
HITECH-What Constitutes a Breach
(exceptions continued)

• Inadvertent disclosures of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity, business associate, or organized healthcare arrangement in which covered entity participates
  – Example: A physician who has authority to use or disclose PHI at a hospital by virtue of participating in an organized health care arrangement (defined by HIPAA rules to mean, among other things, a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. This includes, for example, a covered entity, such as a hospital, and the health care providers who have staff privileges at the hospital) with the hospital is similarly situated (authorized to access PHI) to a nurse or billing employee at the hospital. A physician is not similarly situated to an employee at the hospital who is not authorized to access PHI.
HITECH-What Constitutes a Breach
(exceptions continued)

• If a covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information
  – Example: EOBs are sent to the wrong individuals. A few of them are returned by the post office, unopened as undeliverable. It could be concluded that the improper addresses could not have reasonably retained the information. The EOBs that were not returned as undeliverable, however, and that the covered entity knows were sent to the wrong individuals, should be treated as potential breaches.
HITECH-Breach Notification Obligations

• If a breach has occurred, Tulane will be responsible for providing notice to
  – The affected individuals (without unreasonable delay and in no event later than 60 days from the date of discovery—a breach is considered discovered when the incident becomes known not when the covered entity or Business Associate concludes the analysis of whether the facts constitute a Breach)
  – Secretary of Health & Human Services-HHS- (timing will depend on number of individuals affected by the breach)
  – Media (only required if 500 or more individuals of any one state are affected)
HITECH-Reporting Breaches

• Breaches of unsecured PHI (can include information in any form or medium, including electronic, paper, or oral form) or of any of Tulane’s HIPAA policies and procedures must be reported to the Privacy Official at 504-988-7739 or the Office of the General Counsel immediately.

• Tulane’s policy (GC-026) states,
  – “Any member of the Health Care Component who knows, believes, or suspects that a breach of protected health information has occurred, must report the breach to the Privacy Official or the Office of the General Counsel immediately.”

• If a breach is reported, the incident will be thoroughly investigated.

• The Tulane University Covered Entity is required to attempt to remedy the harmful effects of a breach, including providing notification to affected individuals.
Disciplinary Actions

• Internal Disciplinary Actions
  – Individuals who breach the policies will be subject to appropriate discipline under Policy GC-009
<table>
<thead>
<tr>
<th>Level &amp; Definition of Violation</th>
<th>Example</th>
<th>Action</th>
</tr>
</thead>
</table>
| Accidental and/or due to lack of proper education. | • Improper disposal of PHI.  
• Improper protection of PHI (leaving records on counters, leaving documents in inappropriate areas).  
• Not properly verifying individuals. | • Re-training and re-evaluation.  
• Oral warning with documented discussions of policy, procedures, and requirements. |
| Purposeful violation of privacy or an unacceptable number of previous violations | • Accessing or using PHI without have a legitimate need.  
• Not forwarding appropriate information or requests to the privacy official for processing. | • Re-training and re-evaluation.  
• Written warning with discussion of policy, procedures, and requirements. |
| Purposeful violation of privacy policy with associated potential for patient harm. | • Disclosure of PHI to unauthorized individual or company.  
• Sale of PHI to any source.  
• Any uses or disclosures that could invoke harm to a patient. | Termination. |
Disciplinary Actions

• Civil Penalties
  – Covered entities and individuals who violate these standards will be subject to civil liability.
## Tiered Civil Penalties

<table>
<thead>
<tr>
<th>Circumstance of Violation</th>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity did not know (even with reasonable diligence)</td>
<td>$100 per violation ($25,000 per year for violating same requirement)</td>
<td>$50,000 per violation ($1.5 million annually)</td>
</tr>
<tr>
<td>Reasonable cause, not willful neglect</td>
<td>$1,000 ($100,000)</td>
<td>$50,000 ($1.5 million)</td>
</tr>
<tr>
<td>Willful neglect, but corrected within 30 days</td>
<td>$10,000 ($250,000)</td>
<td>$50,000 ($1.5 million)</td>
</tr>
<tr>
<td>Willful neglect, not corrected</td>
<td>$50,000 ($1.5 million)</td>
<td>None</td>
</tr>
</tbody>
</table>
• An employee who does not report a breach in accordance with the policies and procedures could lose his or her job.
Employee Obligations

- Do not disclose PHI without patient authorization. If you have questions about whether a disclosure is permitted, ask your supervisor.
- If you think there has been an unauthorized disclosure of PHI, contact the Security or Privacy Official or the Office of the General Counsel immediately.
- When removing PHI from Tulane (i.e., by physician removal of medical records or through the use of a laptop), act in accordance with Tulane’s security measures.
Quiz Time!

Download the test, answer the questions, and bring to orientation or email Kim Melerine kmeleri@tulane.edu or fax it to the Student Affairs Office: 504-988-6462

Make sure to retain a confirmation page and/or copy of your submission!